Emergency Management and Response Information Sharing and Analysis Center (EMR-ISAC)

INFOGRAM 17-09 April 30, 2009

NOTE: *This INFOGRAM will be distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures. For further information, contact the Emergency Management and Response- Information Sharing and Analysis Center (EMR-ISAC) at (301) 447-1325 or by e-mail at* emr-isac@dhs.gov.

Swine Flu: First Responder Precautions

As of Thursday morning, 30 April, there are 109 confirmed human infections of the swine flu (i.e., N1H1 virus) in 11 states of the United States according to the Centers for Disease Control and Prevention (CDC). Considering the growth of the influenza virus nationally and internationally, U.S. medical authorities are actively evaluating and advising regarding this national public health emergency.

For the benefit of Emergency Services Sector (ESS) department and agencies, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) assembled recommendations for actions that can be implemented to protect ESS personnel in their performance of duties. These few basic precautions are from the CDC and other first responder sources:

- Review state and local pandemic plans and apply applicable provisions.
- Implement acute febrile respiratory infection screening for all callers or patients with nasal congestion, cough, fever, or other flu-like symptoms.
- Request additional information from the dispatcher when sent to respiratory, sick person, and fever-related calls, but given only limited initial information.
- Perform initial interview of all patients from more than 6 feet away to determine if personal protective equipment precautions are necessary.
- Place a standard surgical mask on all patients with suspected influenza symptoms before approach.
- Maintain strict adherence to hand hygiene by washing with soap and water or alcohol-based hand disinfectant immediately after removing gloves following any contact with patients.
- See more detailed recommendations at the Interim Guidance for Emergency Medical Services (EMS) Systems and 9-1-1 Public Safety Answering Points (PSAPs) for Management of Patients with Confirmed or Suspected Swine-Origin Influenza (H1N1) Infection (http://www.cdc.gov/swineflu/guidance_ems.htm).

The EMR-ISAC offers the following links for more suggestions to protect responders from infection:

- http://www.cdc.gov/flu/swine/recommendations.htm.
- www.pandemicflu.gov.

Nonprofit Organizations: Sources of Funding Assistance

Many American emergency managers and planners have experienced the assistance with food, clothing, and shelter that private nonprofit organizations provide when disaster strikes. However, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) learned that some emergency management agencies received funding from nonprofits to support existing and new programs.

In an article on the Government Technology web site, Adam Stone explained that nonprofits "can tap funding sources unavailable to public agencies, including donations from individuals, corporations, and private foundations. Unlike public agencies, nonprofits are flexible in their ability to use these funds to pursue new programs, and they are free to develop innovative ideas and solicit contributions to support them." Furthermore, "their ability to streamline in times of crisis makes nonprofit partners highly attractive."

The EMR-ISAC verified that emergency management agencies and emergency response departments can readily access broad swaths of the nonprofit community through the National Voluntary Organizations Active in Disaster (NVOAD). NVOAD is an umbrella organization for the major national voluntary agencies that have made disaster-related work their priority. Throughout the year, NOVAD labors to foster cooperation, coordination, communication, and collaboration among the member agencies in order to improve their readiness to effectively respond and work together.

NVOAD Executive Director Diana Rothe-Smith said there's a natural synergy between emergency management and nonprofit capabilities. She further asserted that voluntary organizations active in disasters can be "strong advocates for nonprofit involvement, and they often have a prominent place at the table." NVOAD contact information can be seen at the following link: http://www.nvoad.org/Contact/tabid/55/Default.aspx.

Cell-Phone Tapping

Emergency Services Sector (ESS) personnel use cellular (cell) phones extensively on and off duty and for personal use. The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) has reported on emergencies when responders had to rely on cell phones because other forms of communication had been disrupted or degraded. As indispensable as cell phones have become in everyday life and in the workplace, they also present an information and operations security vulnerability for emergency departments and organizations.

Cell phones operate using radio waves which are easily intercepted with a radio receiver. Among the multitude of gadgets, tools, and weapons available via the Internet are cell phone spying devices that can accomplish cell phone tapping noninvasively. Cell phone vulnerabilities include conversation monitoring while the phone is in use, the phone being turned into a microphone to monitor conversations in the vicinity while the phone is inactive, and cloning, i.e., the use of the phone's number by others to make calls (experts point out that pagers are similarly vulnerable and pager messages can be monitored). It is illegal to intercept cell phone calls, but it can be accomplished relatively easily and is virtually undetectable.

In examining this threat to the communications/cyber critical infrastructures of the ESS, the EMR-ISAC examined a number of resources, including several from WTHR News in Indianapolis, which reported on a family stalked for months by a cell phone spy. The stalking eventually ended after the police and FBI became involved, but the perpetrator was never identified. Based on advice from cyber forensics experts and investigators featured on a WTHR video, and from other sources, the EMR-ISAC compiled the following precautions for responder departments and agencies:

- Do not carry a cellular phone into classified areas or areas where sensitive discussions are held because a cell phone can be turned into a microphone without the owner's knowledge.
- Turn cell phones on only when placing a call. Experts encourage removing the battery whenever the phone is not in use.
- Do not discuss sensitive information on cell phones. Explain that the phone is vulnerable to monitoring and that the conversation must be limited to non-sensitive information.
- Do not leave cell phones unattended and therefore vulnerable to having spy software downloaded.
- Turn off vehicle-mounted cell phones before allowing parking attendants access to the car, even if the phone locks automatically when the ignition is turned off.
- Avoid using cell phones near airports, stadiums, malls, or other heavy traffic locations where scanners might be used for random monitoring.
- Opt to use a personal identification number (PIN) if available from your cellular service company.
- Choose a cell phone that is not Internet-accessible. Some spy software won't work on basic cell phones that limit the ability of others to download certain types of spyware onto the phone.
- Consider making sensitive phone calls on a newly purchased cell phone that comes with a pre-paid month-to-month service plan.
- Understand that once spy software is on a phone, a secret pass code is required to deactivate the program.

- Watch for signs that could suggest a cell phone is being secretly tapped: cell phone battery is warm even when phone has not been used; phone lights up at unexpected times, including occasions when phone is not in use; and, there are unexpected beeps or clicks during phone conversations.

For additional information, see the resources at http://www.wthr.com/Global/story.asp?s=9346833.

ESS Not Given Chemical Information

In August 2008, a large explosion and fire killed two workers and injured eight others (six were first responders) at the Bayer CropScience chemical plant in Institute, West Virginia. This month, the Committee on Energy and Commerce of the U.S. House of Representatives released the results of "Secrecy in the Response to Bayer's Fatal Chemical Plant Explosion," a hearing conducted by its Subcommittee on Oversight and Investigations. Of significance to the nation's Emergency Services Sector (ESS) is the subcommittee's finding that, "Bayer failed to provide emergency responders with critical information about the scope of the explosion, the potential chemical hazards involved, or the actions needed to safeguard the surrounding community," in effect engaging "in a campaign of secrecy."

While researching the incident, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) learned that the blast was caused by a thermal runaway reaction during the production of a pesticide, and "likely resulted from significant lapses in chemical process safety management at the plant," according to findings by U.S. Chemical Safety Board (CSB) investigators.

CSB Chairman John Bresland explained: "The explosion occurred within 80 feet of a pressure vessel containing more than 13,000 pounds of methyl isocyanate, or MIC, a raw material for the pesticide the company was making at the time, and the same chemical that caused death and injury in the Bhopal accident 25 years ago." The U.S. Environmental Protection Agency describes MIC as extremely toxic to humans from acute exposure. The Bayer facility is the only plant in the nation that still produces large amounts of MIC, yet the information had not been shared with responders who needed it to make critical planning and operations decisions such as whether to order evacuations or sheltering in place.

Equipment deficiencies, procedural deviations, worker fatigue, and lack of training on brand-new computerized control equipment were other factors that contributed to the accident. Extensive documentation--testimony, photographs, videos, incident critique notes, and after-action reports--is available at the House Committee's web site. Also at the link under "Emergency Response Documents" are verbatim transcripts of calls between Bayer CropScience and Metro 9-1-1, and testimony from local chief officers who described hearing and feeling the explosion, seeing the fire(s) and then attempting to respond using their knowledge, training, and procedures, and protect their personnel, citizens, and community, all while repeatedly being deprived of information and access. (http://energycommerce.house.gov/index.php?option=com_content&view=article&id=1583&catid=133&itemid=73)

DISCLAIMER OF ENDORSEMENT

The U.S. Fire Administration/EMR-ISAC does not endorse the organizations sponsoring linked web sites, and does not endorse the views they express or the products/services they offer.

FAIR USE NOTICE

This INFOGRAM may contain copyrighted material that was not specifically authorized by the copyright owner. EMR-ISAC personnel believe this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

REPORTING NOTICE

The National Infrastructure Coordinating Center (NICC) within the Department of Homeland Security (DHS) Office of Infrastructure Protection is the central point for notifications regarding infrastructure threats, disruptions, intrusions, and suspicious activities. Emergency Services Sector personnel are requested to report any incidents or attacks involving their infrastructures using at least the first and second points of contact seen below:

1) NICC - Voice: 202-282-9201, Fax: 703-487-3570, E-Mail: nicc@dhs.gov
2) Your local FBI office - Web: *http://www.fbi.gov/contact/fo/fo.htm*
3) EMR-ISAC - Voice: 301-447-1325, E-Mail: *emr-isac@dhs.gov*, fax: 301-447- 1034,
Web: *www.usfa.dhs.gov/subjects/emr-isac*, Mail: J-247, 16825 South Seton Avenue,
Emmitsburg, MD 21727